



FortiAnalyzer

Au cours de cette session d'une journée, vous apprendrez à utiliser FortiAnalyzer.

Vous explorerez l'interface d'administration, inscrirez de nouveaux équipements et collecter des logs de manière centralisée. Puis vous manipulerez les logs et les archives, les rapports existants et configurerez des rapports personnalisés. A l'issue de cette formation, vous aurez une solide compréhension du FortiAnalyzer et saurez comment le déployer dans des environnements simples ou complexes.

Au cours des labs, vous pourrez également effectuer une analyse forensique de logs basés sur une attaque réseau simulée, et étudierez les solutions à des problèmes courants de configuration.

Version de l'OS

FortiAnalyzer 6.2

Format du cours

- Instructeur présentant les modules.
- Exercices pratiques à la fin de chaque module.

Centre de formation Agréé Fortinet

Vous former dans un centre de formation agréé Fortinet vous assure le meilleur niveau de maîtrise de vos équipements Fortinet.

Agenda

1. Introduction et configuration initiale
2. Administration et Gestion
3. Enregistrement d'équipements
4. Logs
5. Rapports

Objectifs

A l'issue de cette session de deux jours vous serez en mesure de :

- Décrire les fonctionnalités clés du FortiAnalyzer
- Choisir et déployer
- Déployer des ADOMs pour gérer des environnements multi-clients au sein d'un même FortiAnalyzer
- Configurer le RAID
- Inscrire des devices supportés
- Diagnostiquer des problèmes de configuration
- Gérer les quotas de disques
- Gérer les devices inscrits
- Protéger les informations de logs
- Visualiser les logs
- Chercher des évènements dans les logs
- Générer des rapports personnalisés
- Personnaliser des graphes et des sets de données
- Gérer les rapports
- Diagnostiquer des rapports

A qui s'adresse cette formation

A tous ceux qui administrent régulièrement des FortiAnalyzer, ainsi que des logs de FortiGates

Prérequis

- Bonne connaissance des contenus de la formation *FortiGate Security* et *FortiGate Infrastructure*
- Une connaissance de la syntaxe de SQL est un plus.

Prérequis techniques

- Sauf précision contraire : aucun, des postes sont fournis sur les sites de formation à Paris et Lyon

Certification

Cette formation permet, avec la formation FortiManager de se préparer au passage de la certification NSE5.